NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

HPCC Program

IT Security Plan

Issue Date:
June 14, 2000

HIGH PERFORMANCE COMPUTING AND COMMUNICATIONS PROGRAM

IT SECURITY PLAN

Approved by:

____

Eugene L. Tu
HPCC Program Manager
Ames Research Center

____

William R. Van Dalsem
HPCC Deputy Program Manager
Ames Research Center

Concurred by:

Catherine Schulbach, Project Manager
Computational Aerospace Sciences

James Fischer, Project Manager
Earth and Space Sciences

Robert Ferraro, Project Manager
Remote Exploration and Experimentation

Kenneth Freeman, Project Manager
NASA Research and Education Network

Mark Leon, Project Manager
Learning Technologies

Daniel S. Katz, Lead
Application Integration Management Team

Jerry C. Yan, Lead
System Software Integration Management Team

Raphael R. Some, Lead
Testbed Integration Management Team

HIGH PERFORMANCE COMPUTING AND COMMUNICATIONS PROGRAM

IT SECURITY PLAN

Table of Contents

IT SECURITY PLAN
HIGH PERFORMANCE COMPUTING AND COMMUNICATIONS (HPCC)

INTRODUCTION AND PROGRAM BACKGROUND

1.1 Introduction

This document is the IT Security Plan for the NASA High Performance Computing and Communications (HPCC) Program. This is the controlling document that defines the top-level IT security plans for the HPCC Program. This IT Security Plan is compliant with the IT security requirements of NASA Programs as defined in NASA NPG 2810.1, Section 2.4.1.

1.2 Program Background

The goal of the NASA HPCC Program is to:

> ***Accelerate the development, application, and transfer of high-performance computing and computer communications technologies to meet the engineering and science needs of the U.S. aerospace, Earth and space science, spaceborne research, and education communities, and to accelerate the distribution of these technologies to the American Public.***

Applications in the areas of Earth science, space science, aerospace technology, and education are used as drivers of HPCC's computational and communications technology research, providing the requirements context for the work that is done.

As a cross-cutting multi-enterprise initiative, the HPCC Program receives funds from the Aerospace Technology (AT), Space Science (SS), and Earth Science (ES) Enterprises, and the Office of Human Resources and Education.

The HPCC Program is coordinated through the Aerospace Technology Enterprise and is managed by NASA Ames Research Center. The Program has supporting work at nine NASA field centers and the Jet Propulsion Laboratory (JPL) and is organized into five Projects:

- Computational Aerospace Sciences (CAS)
- Earth & Space Sciences (ESS)
- Remote Exploration and Experimentation (REE)
- Learning Technologies (LT)
- NASA Research and Education Network (NREN)

Further information regarding the HPCC Program and Projects may be found in the HPCC PCA, Program Plans, and Project Plans.

SCOPE

2.1 Scope of NASA HPCC Program IT Security Plan

In compliance with NASA's IT security requirements, this HPCC IT Security Plan:

1. Identifies the primary HPCC IT systems

2. Identifies and characterize IT security risks

3. Identifies risk reduction and contingency plans that address the high risk exposure IT security risks

All medium and low risk exposure IT security risks identified in this document, or identified in Project-level documentation, may be addressed in either this document or Project-level documentation.

PRIMARY SYSTEM IDENTIFICATION

3.1 Primary Systems

The primary IT systems currently used within the HPCC Program are identified in Table 1:

System	HPCC Projects Using System	Performing Organization Responsible for Maintaining System IT Security
Lomax (512-Processors SGI Origin)	CAS ESS	Numerical Aerospace Simulation Systems Division NASA Ames Research Center IT Security POC: David Tweten
Steger (256-Processors SGI Origin)	CAS ESS	Numerical Aerospace Simulation Systems Division NASA Ames Research Center IT Security POC: David Tweten
Hopper (64-Processors SGI Origin)	CAS ESS	Numerical Aerospace Simulation Systems Division NASA Ames Research Center IT Security POC: David Tweten
Sharp (24-processor SGI Origin)	CAS	NASA Glenn Research Center Computer Service Division IT Security POC: Kimberly Johnson
Whitcomb (16-processor SGI Origin)	CAS	NASA Langley Research Center Computational Aerosciences Team IT Security POC: Dave Rudy
Mass Storage System (680 Petabytes of StorageTek Robots)	CAS ESS	Numerical Aerospace Simulations Systems Division NASA Ames Research Center IT Security POC: David Tweten
Jsimpson (1380-Processor Cray T3E)	ESS	Earth and Space Data Computing Division NASA Goddard Space Flight Center IT Security POC: Pat Gary
theHive (255-Processor Beowulf Cluster)	ESS	Earth and Space Data Computing Division NASA Goddard Space Flight Center IT Security POC: Pat Gary
REE Level Zero Testbed (11-Node PowerPC Cluster)	REE	Avionic Equipment Section (344) NASA Jet Propulsion Laboratory IT Security POC: John M. Davidson
REE First Generation Testbed	REE	Avionic Equipment Section (344)

(20-Node PowerPC System with High-Bandwidth Low-Power Interconnect)		Jet Propulsion Laboratory IT Security POC: John M. Davidson

Table 1: Primary HPCC IT Systems (continued).

System	**HPCC Projects Using System**	**Performing Organization Responsible for Maintaining System IT Security**
NREN Backbone	NREN	Numerical Aerospace Simulation Systems Division NASA Ames Research Center IT Security POC: Dave Guevara
LT LEARN Web Server (Sun Solaris Server)	LT	HPCC-LT NASA Ames Research Center IT Security POC: Alan Federman

Table 1: Primary HPCC IT Systems (concluded).

IT security risks identified in the following section are primarily related to the above systems or ancillary systems which support the use of these systems.

IT SECURITY RISKS

4.1 IT Security Risk Identification and Classification

Risks to each appropriate category of IT resources (as defined by NASA NPG 2810.1) are identified and classified in Table 3. The impact and probability of each risk to each of the HPCC Projects is presented.

The impact of a risk is considered to be the impact to the overall program goal and objectives if the risk event were to occur. The probability of a risk is estimated in view of the state of current information technologies, community-wide standard IT security practices, and the estimated likelihood that parties will access and/or damage resources or events will damage resources.

A total risk exposure is assigned based on the risk impact and risk probability as follows:

Impact-Probability Values	**Total Risk Exposure**
High-High High-Medium Medium-High	High
High-Low Medium-Medium Low-High	Medium
Medium-Low Low-Medium Low-Low	Low

Table 2: Evaluation of total risk exposure.

IT Resource	Risk	Project	Risk Impact	Risk Probab-ility	Total Risk Exposure	Explanations
Data and Information	Inappropriate data access	CAS	High	High	High	CAS application work includes data which may be proprietary, competitively sensitive, or restricted via ITAR or EAR regulations.
		ESS	Medium	Medium	Medium	ESS application work includes data which may be competitively sensitive in an academic setting.
		REE	Low	Medium	Low	REE has no "data" per se, except perhaps some proprietary vendor information, although this asset largely falls under "software"
		NREN	Medium	Low	Low	NREN has network configuration data that could include non-disclosure vendor information
		LT	Low	Low	Low	LT educational content is generally publicly accessible
	Data loss or corruption	CAS	High	Medium	High	CAS applications perform large computations that could be difficult to reproduce
		ESS	Medium	Medium	Medium	ESS applications perform large computations that could be difficult to reproduce.
		REE	Low	Medium	Low	See comments under "Inappropriate Data Access"
		NREN	Medium	Medium	Medium	NREN has network management and network configuration data that could be difficult to reproduce
		LT	Medium	Medium	Medium	LT educational content archives could be difficult to reproduce

Table 3: Risk identification and evaluation (continued).

IT Resource	**Risk**	**Project**	**Risk Impact**	**Risk Probab-ility**	**Total Risk Exposure**	**Explanations**
Software and Firmware	Inappropriate software or firmware access	CAS	High	High	High	CAS application and systems software include software which may be proprietary, competitively sensitive, or restricted via ITAR or EAR regulations.
		ESS	Medium	Medium	Medium	ESS application and systems software include software which may be competitively sensitive in an academic setting.
		REE	High	Medium	High	REE Software includes ITAR and competition sensitive assets.
		NREN	Medium	Medium	Medium	NREN applications come with licensing restrictions
		LT	Low	Medium	Low	LT applications come with licensing restrictions for numbers of users
	Software or firmware loss or corruption	CAS	Medium	Low	Low	Loss of software or firmware may make computer systems difficult or impossible to use until the software is recreated, rebuilt, or reinstalled.
		ESS	Medium	Low	Low	Loss of software or firmware may make computer systems difficult or impossible to use until the software is recreated, rebuilt, or reinstalled.
		REE	High	Medium	High	Permanent loss of REE software (e.g., SIFT components) could be devastating to the project.
		NREN	Medium	Low	Low	NREN uses primarily adapted COTS which can be restored, albeit with some delay
		LT	Medium	Low	Low	LT uses primarily adapted COTS which can be restored, albeit with some delay

Table 3: Risk identification and evaluation (continued).

IT Resource	Risk	Project	Risk Impact	Risk Probab-ility	Total Risk Exposure	Explanations
Communi-cation equipment	Inappropriate communication equipment access	CAS	High	Medium	High	Communications could be degraded or lost, or sensitive data could be compromised.
		ESS	Low	Medium	Low	Communications could be degraded or lost, or sensitive data could be compromised.
		REE	Low	Low	Low	(For system security breaches, see "Computers and Ancillary Equipment")
		NREN	High	Medium	High	NREN has network configuration data that could include non-disclosure vendor information
		LT	Low	Low	Low	Physical security and access control systems are in place
	Communication equipment failure	CAS	High	Medium	High	Ability to access computer systems could be lost, delaying work.
		ESS	Medium	Medium	Medium	Ability to access computer systems could be lost, delaying work. Most ESS Investigators are external to NASA centers and depend on network access to attain ESS goals.
		REE	High	Low	Medium	REE has a large community of external users, both for development of applications and of system software and tools. External access is vital to their participation and to the attainment of project goals.
		NREN	High	Medium	High	NREN R&D is highly-dependent on network availability, other than short term inaccessibility could delay project deliverables
		LT	High	Medium	High	LT is highly-dependent on network availability, other than short term inaccessibility could impact outreach activities

Table 3: Risk identification and evaluation (continued).

IT Resource	Risk	Project	Risk Impact	Risk Probab-ility	Total Risk Exposure	Explanations
Computers and ancillary equipment	Inappropriate computer access	CAS	High	Medium	High	Inappropriate computer access could result in inappropriate access to, corruption of, or loss of data and software.
		ESS	Medium	Medium	Medium	Inappropriate computer access could result in inappropriate access to, corruption of, or loss of data and software.
		REE	High	Medium	High	Inappropriate access could result in a violation of ITAR restrictions or the dissemination of competition sensitive software and information.
		NREN	Low	Low	Low	Inappropriate access could result in a violation of vendor non-disclosure agreements
		LT	Low	Low	Low	Physical security and access control systems are in place
	Computer equipment degradation or failure	CAS	Medium	Medium	Medium	Failure of computer equipment could result in significant delays in work.
		ESS	High	Low	Medium	Failure of computer equipment could result in significant delays in work.
		REE	High	Low	Medium	Failure of computer equipment could cause significant delays in the project. Fortunately, the probability of this is low.
		NREN	Low	Low	Low	Failure of computer equipment could cause significant delays in the project.
		LT	Low	Low	Low	LT uses standard, replaceable hardware and ancillary equipment

Table 3: Risk identification and evaluation (continued).

IT Resource	Risk	Project	Risk Impact	Risk Probab-ility	Total Risk Exposure	Explanations
Facilities that house IT resources	Inappropriate facility access	CAS	Medium	Medium	Medium	Inappropriate facility access could result in damage to equipment, and possibly data and software. Loss of equipment, data, or software would impact work schedule.
		ESS	Medium	Medium	Medium	Inappropriate facility access could result in damage to equipment, and possibly data and software. Loss of equipment, data, or software would impact work schedule.
		REE	Medium	Low	Low	The probability of inappropriate access is low.
		NREN	Medium	Medium	Medium	NREN has network configuration and vendor software data that could include non-disclosure vendor information
		LT	Medium	Medium	Medium	LT product dissemination could be halted or slowed by inappropriate access
	Facilities damaged or destroyed	CAS	High	Low	Medium	Damage or destruction of computer facilities would cause major disruption in performance of work, causing significant delays.
		ESS	High	Low	Medium	Damage or destruction of computer facilities would cause major disruption in performance of work, causing significant delays.
		REE	High	Low	Medium	Destruction of testbed equipment would cause unrecoverable loss. However, the probability, e.g., of fire, flooding, etc., is small.
		NREN	Low	Low	Low	Destruction of testbed equipment would cause unrecoverable loss.
		LT	Low	Low	Low	LT can be served from alternate NASA Centers

Table 3: Risk identification and evaluation (concluded).

IT SECURITY RISK REDUCTION AND CONTIGENCY POLICIES

5.1 Risk Reduction and Contingency Approaches

Risk reduction strategies of any IT security risk identified as having a total risk exposure of "High" are presented in this Program-level document. All remaining risk identified in this document, or identified in Project-level documentation, may be addressed in either this document or Project-level documentation.

In accordance with NPG 2810.1, program management is responsible for identifying IT security risks and insuring that performing organizations and line-management have implemented procedures to reduce these risks. Risk reduction policies and activities are, therefore, primarily captured in the IT security plans maintained by the performing organizations.

In addition, performing organization contingency policies and activities are identified for each risk. Contingency policies and activities describe arrangement that have been made and the steps that will be taken to continue system operations in the event of risk occurrence.

5.2 Risk Reduction and Contingency Policies and Activities Identification

The mapping of identified risks to risk reductions and contingency policies and activities is presented in Table 4:

IT Resource	Risk	Project	Total Risk Exposure	Risk Reduction Policies and Activities	Contingency Policies and Activities
Data and Information (continued)	Inappropriate data access	CAS	High	Security model developed and implemented. Systems isolated from web access, password protection, systems monitoring/scanning, publication and enforcement of security policies. Access by non-US citizens screened.	NAS Policy 16—Incident Response. Policy 16: requires that we investigate potential compromises sufficiently to determine that they really are compromises, that we then call in Code JT and the Inspector General to collect evidence, and that we not re-install the software and put the machine back on the net until they are done with it.
		ESS	Medium	Security model developed and implemented. Systems isolated from web access, password protection, systems monitoring/scanning, publication and enforcement of security policies. Access by non-US citizens screened.	Recover as described in GSFC Code 930 AIS Contingency Plan, May 2000, especially Section 4.1 and Appendix A.
		REE	Low	Data will be protected by restricting access to REE facilities and testbeds.	The cause of the inappropriate access will be identified and preventive measures will be taken against future breaches.
		NREN	Low	Data will be protected by restricting access to NREN facilities and testbeds.	The cause of the inappropriate access will be identified and preventive measures will be taken against future breaches.
		LT	Low	Educational outreach data is publicly accessible. System administrators are trained to observe "unusual" accesses	LT reports any unusual access to the Operations Center and restores from last back-up or archive when authorized to.

Table 4: Risk reduction and contingency policy and activities identification (continued).

IT Resource	Risk	Project	Total Risk Exposure	Risk Reduction Policies and Activities	Contingency Policies and Activities
Data and Information (concluded)	Data loss or corruption	CAS	High	Adherence to operational procedures, routine performance of backups, safe storage of backup data, monitoring, and preventive maintenance of equipment.	Restoration from backups.
		ESS	Medium	Adherence to operational procedures, routine performance of backups, safe storage of backup data, monitoring, and preventive maintenance of equipment.	Restore from backups as described in GSFC Code 930 AIS Contingency Plan, May 2000, especially Section 4.3.
		REE	Low	Data will be protected by routine backups and safe storage of backups.	Data will be restored from the most recently backed up archival storage.
		NREN	Medium	Data is protected by routine backups and safe storage of backups.	Restore from last back-up
		LT	Medium	Back-ups and archiving	Restore from last back-up

Table 4: Risk reduction and contingency policy and activities identification (continued).

IT Resource	**Risk**	**Project**	**Total Risk Exposure**	**Risk Reduction Policies and Activities**	**Contingency Policies and Activities**
Software and Firmware (continued)	Inappropriate software or firmware access	CAS	High	Security model developed and implemented. Systems isolated from web access, password protection, systems monitoring/scanning, publication and enforcement of security policies. Access by non-US citizens screened.	NAS Policy 16—Incident Response. Policy 16: requires that we investigate potential compromises sufficiently to determine that they really are compromises, that we then call in Code JT and the Inspector General to collect evidence, and that we not re-install the software and put the machine back on the net until they are done with it.
		ESS	Medium	Security model developed and implemented. Systems isolated from web access, password protection, systems monitoring/scanning, publication and enforcement of security policies. Access by non-US citizens screened.	Recover as described in GSFC Code 930 AIS Contingency Plan, May 2000, especially Section 4.1 and Appendix A.
		REE	High	ITAR and competition sensitive items will be protected by restricting access to REE facilities and to the REE testbed.	The cause of the inappropriate access will be identified and preventive measures will be taken against future breaches.
		NREN	Medium	Software and firmware items will be protected by restricting access to NREN facilities and to the NREN testbed	The cause of the inappropriate access will be identified and preventive measures will be taken against future breaches.
		LT	Low	System software and firmware are protected by user access controls.	Report unusual access to the Operations Center Restore software or firmware based on back-ups or sparage when authorized to.

Table 4: Risk reduction and contingency policy and activities identification (continued).

IT Resource	**Risk**	**Project**	**Total Risk Exposure**	**Risk Reduction Policies and Activities**	**Contingency Policies and Activities**
Software and Firmware (concluded)	Software or firmware loss or corruption	CAS	Low	Adherence to operational procedures, routine performance of backups, safe storage of backup data, monitoring, and preventive maintenance of equipment.	Restoration from backups.
		ESS	Low	Adherence to operational procedures, routine performance of backups, safe storage of backup data, monitoring, and preventive maintenance of equipment.	Restore from sources as described in GSFC Code 930 AIS Contingency Plan, May 2000, especially Section 4.3.
		REE	High	Routine backups will be performed and archival copies kept of all project-critical software and firmware.	Software will be restored from the most recently backed up archival copies.
		NREN	Low	Routine backups will be performed and archival copies kept of all project-critical software and firmware.	Software will be restored from the most recently backed up archival copies.
		LT	Low	Use of Common Off The Shelf (COTS) software	Restore software or firmware

Table 4: Risk reduction and contingency policy and activities identification (continued).

IT Resource	Risk	Project	Total Risk Exposure	Risk Reduction Policies and Activities	Contingency Policies and Activities
Communication equipment (continued)	Inappropriate communication equipment access	CAS	High	Restricted access to facilities, configuration management processes.	Network traffic patterns are constantly monitored. When scans or denial of service attacks are detected, we activate perimeter router packet filters.
		ESS	Low	Restricted access to facilities, configuration management processes.	Network traffic patterns are constantly monitored. When scans or denial of service attacks are detected, we activate perimeter router packet filters.
		REE	Low	Communication equipment will be protected by restricting access to REE facilities.	The cause of the inappropriate access will be identified and preventive measures will be taken against future such access.
		NREN	High	NREN Configuration Management Procedures	The cause of the inappropriate access will be identified and preventive measures will be taken against future breaches.
		LT	Low	Physical security and access control of equipment is in place.	LT reports any observed access to Security, and when approved, restores or replaces equipment.

IT Resource	Risk	Project	Total Risk Exposure	Risk Reduction Policies and Activities	Contingency Policies and Activities
Communi-cation equipment (concluded))	Communication equipment failure	CAS	High	Maintenance agreements, backup equipment, configuration management, preventive maintenance.	Operational procedures invoked, event escalation plans implemented.
		ESS	Medium	Maintenance agreements, backup equipment, configuration management, preventive maintenance.	Restore as described in GSFC Code 930 AIS Contingency Plan, May 2000, especially Section 4.3.
		REE	Medium	External users may have their own hardware systems that can be used temporarily in lieu of access to the REE testbed.	Hardware development systems consisting of a few nodes can be shipped on loan within days to impacted external users.
		NREN	High	NREN Configuration Management Procedures	Communications equipment components can be shipped on loan within days to support impacted users
		LT	High	Load distribution	Service from another site

Table 4: Risk reduction and contingency policy and activities identification (continued).

IT Resource	Risk	Project	Total Risk Exposure	Risk Reduction Policies and Activities	Contingency Policies and Activities
Computers and ancillary equipment (continued)	Inappropriate computer access (continued)	CAS	High	SSH/OPIE Project Restricted access to center and card key protection of computer facilities. Security model developed and implemented. Systems isolated from web access, password protection, systems monitoring/scanning, publication and enforcement of security policies. Access by non-US citizens screened. SSH/OPIE project plan exists in the directory, lou:~tweten/Ssh_Project either as sshplan.pdf or sshplan.ps.	NAS Policy 16 – Incident Response NAS Policy 16 exists at: http://in.nas.nasa.gov/Groups/Security/policies/IG/incidents.html
		ESS	Medium	Restricted access to center and card key protection of computer facilities. Security model developed and implemented. Systems isolated from web access, password protection, systems monitoring/scanning, publication and enforcement of security policies. Access by non-US citizens screened.	Recover as described in GSFC Code 930 AIS Contingency Plan, May 2000, especially Section 4.1 and Appendix A.
		REE	High	Access is password controlled. Access by non-U.S. citizens is granted only following review and approval by the JPL Foreign Affairs Office. Sensitive data/ software is firewalled.	In case of an inappropriate access, all access may be cut off until a corrective measure is determined and implemented.

Table 4: Risk reduction and contingency policy and activities identification (continued).

IT Resource	Risk	Project	Total Risk Exposure	Risk Reduction Policies and Activities	Contingency Policies and Activities
Computers and ancillary equipment (concluded)	Inappropriate computer access (concluded)	NREN	Low	NREN Computer Systems have restricted user access.	The cause of the inappropriate access will be identified and preventive measures will be taken against future breaches.
		LT	Low	LT has physically secured hardware and computer equipment.	LT Staff members are trained to observe unusual conditions. We report any of these observations to the Operations Center and continue work, repair or replace equipment when authorized to.
	Computer equipment degradation or failure	CAS	Medium	Maintenance Contracts, configuration management, preventive maintenance.	Operational procedures invoked, event escalation plans implemented.
		ESS	Medium	Maintenance Contracts, configuration management, preventive maintenance.	Restore as described in GSFC Code 930 AIS Contingency Plan, May 2000, especially Section 4.3.
		REE	Medium	Proper environmental conditions will be maintained and spares of critical components will be kept in stock. Alternate hardware is available through the Level Zero Testbed.	Failed components will be replaced. The conditions that led to the failure will be corrected. Users may temporarily move operations to the Level Zero Testbed.
		NREN	Low	Proper environmental conditions will be maintained and spares of critical components will be kept in stock.	Failed components will be replaced. The conditions that led to the failure will be corrected.
		LT	Low	LT performs periodic tests of activity and performance.	Service from another site while repairing or replacing as necessary.

Table 4: Risk reduction and contingency policy and activities identification (continued).

IT Resource	**Risk**	**Project**	**Total Risk Exposure**	**Risk Reduction Policies and Activities**	**Contingency Policies and Activities**
Facilities that house IT resources (continued)	Inappropriate facility access	CAS	Medium	Restricted access to center and card key protection of computer facilities.	Staff members are encouraged to challenge unfamiliar or unbadged people in secured areas, and to call Center security if a challenge seems unwise or if they don't get a satisfactory response. All HPCC computers are kept in secured areas. Outside normal business hours the whole building becomes a secured area, providing a buffer.
		ESS	Medium	Restricted access to center and card key protection of computer facilities.	Recover as described in GSFC Code 930 AIS Contingency Plan, May 2000, especially Section 4.1 and Appendix A.
		REE	Low	The JPL Oak Grove Facility is guard protected and the REE laboratory is locked after business hours.	The circumstances that led to the inappropriate access will be corrected.
		NREN	Medium	All NREN communications facilities are guard protected and locked at all times	The circumstances that led to the inappropriate access will be corrected.
		LT	Medium	Facilities have physical security and access controls in place.	Service from another site

Table 4: Risk reduction and contingency policy and activities identification (continued).

IT Resource	Risk	Project	Total Risk Exposure	Risk Reduction Policies and Activities	Contingency Policies and Activities
Facilities that house IT resources (concluded)	Facilities damaged or destroyed	CAS	Medium	Routine backups of data and software. All required and reasonable safety and security precautions imp lements.	NAS Disaster Recovery Plan
		ESS	Medium	Routine backups of data and software. All required and reasonable safety and security precautions implemented.	Restore as described in GSFC Code 930 AIS Contingency Plan, May 2000, especially Section 4.3.
		REE	Medium	All required and reasonable safety and security precautions will be taken.	Alternative facilities will be identified and utilized while damaged facilities are repaired.
		NREN	Low	Usage of alternate facilities	Alternative facilities will be identified and utilized while damaged facilities are repaired.
		LT	Low	Alternate facilities	Service from another site

Table 4: Risk reduction and contingency policy and activities identification (concluded).

IT SECURITY PLAN REVIEW AND UPDATE

The NASA HPCC Program IT Security Plan will be updated at least annually to reflect current IT resources, risks, and risk reduction and contingency policies and activities.